ITS
Office of Information Technology Services

Service Level Agreement for Information Security Threat Management and Incident Response Services

Contents

1 Executive Summary

Information Security Threat Management and Incident Response Services are offered to help state agencies to safeguard citizens data, to meet the requirements of the security standards legislation, **N.C.G.S. § 147-33.110-33.113 and N.C.G.S. § 147-33.72c,** and other legal and regulatory requirements. These services support agency efforts to implement an information security program by enabling an agency to quickly react to real and potential cyber security incidents. Services include security consulting, training, and support to help the agency identify and mitigate security risks by defining, implementing, testing, and maintaining a cyber security incident plan for its automated business systems. The agency benefits from the integration of the statewide and agency level cyber security incident plans. The North Carolina Information Sharing and Analysis Center, NCISAC, operated by the ITS Information Security Office, ISO, is part of the Multi State Information Sharing and Analysis Center, MSISAC, formed by the network of such centers in each state and in the Federal Department Of Homeland Security. These centers share and distribute cyber information on cyber security vulnerabilities, threats, warnings and risk mitigation measures to all participants. This makes some of the best and most timely cyber security information available to the agency. Using these services enables an agency to be an active participant in the integration of agency, state and national level security cyber security incident and threat management processes. The agency benefits from an informed approach to threat management and gains an increased understanding and awareness of information security vulnerabilities that improves an agency's overall security posture.

2 Service Provided, Availability and Support

2.1 Service Objective

This Service Level Agreement (SLA) documents Information Security Threat and Vulnerability Management Services provided by ITS Information Security Office (ISO) for an agency. The ultimate objective of this Agreement is to document the support and processes necessary to ensure high-quality and timely delivery of this service. This document clarifies all parties' responsibilities and procedures to ensure Customer needs are met in a timely manner. Although the SLA is in the form of a document that defines a level of service, the desired outcome is to provide a clear understanding and expectation of the service ITS provides and to work with the customer as a business partner to improve and optimize the business as well as improve ITS services.

2.2 Service

- Threat Management
  - Provide notifications to appropriate agency staff, security liaisons and members of the security distribution list concerning new viruses, worms, and other threats to the health of the state's network.
  - Provide notifications to agency security liaisons and members of the security distribution list concerning vulnerabilities in widely deployed operating systems and applications.

- North Carolina Information Sharing and Analysis Center (NC-ISAC).
  - Coordination of governmental security operations throughout the state and nation.
  - Integration with other states and the Department of Homeland Security as part of the Multi-state Information Sharing and Analysis Center (MS-ISAC).
  - Cyber incident management and forensic support activities.
  - Statewide cyber security incident response plan.
  - Integration of agency incident plans with statewide incident plan.
  - Confidential communications through the ISO Security Portal.

- Security Consulting
  - Assist agencies with analysis, resolution and maintenance of Information Technology risks, threats, vulnerabilities and protection requirements.
  - Provide follow-up consultation in response to audit and/or security assessment findings.
  - Review agency incident management plans

- Security Training
  - Train and assist agency with development and maintenance of agency incident management plans
  - Provide incident management plan response training

ITS agrees to provide technical support regarding technical questions or problems with all services documented.

2.3 Services Out of Scope

None at this time.

2.4 Hours of Availability

The service described in this SLA is available from 7*:00 a.m. to 6:00 p.m*. *Monday through Friday* eastern time (except on state holidays).

2.5 Hours of Support

The support for this SLA is available as follows:
Regular Staff Schedule as noted in section 2.4
On-Call Schedule/Hours as required for emergencies and after hours scheduled work

2.6 Constraints on Availability

Scheduled Maintenance Windows:
In the event the consultation engagement involves performance of vulnerability or port scanning, the scanning activity will be conducted within customer maintenance window unless other arrangements are made.

Emergency Maintenance Windows:
Emergency Maintenance windows will be handled through the urgent change process.

2.7 Contacting Support

Call the Customer Support Center (CSC) at **919-754-6000** or toll free at **1-800-722-3946**
-or –
Email the CSC at ITS.Incidents@ncmail.net

2.8 Customer Support Center Response Times

The following priority chart shows response time after initial Assessment/Assignment, creation of iWise ticket by the Customer Support Center, and acknowledgement of the ticket to the customer, including the provision of a ticket number. Times are measured in clock hours and/or minutes unless otherwise specified. If a ticket is initiated by a telephone call, it will be created within 10 minutes; if initiated by email, the ticket will be processed within 30 minutes.

Target Incident Response Time:
The time the Second Level support has to begin to actively work a ticket.

Target Status Update Time:
The time interval the assigned group / ticket owner has to update the ticket.

Target Customer Notification Time
The interval that the Customer Support Center has to update the customer on ticket status.

Target Resolution Time:
The total time from ticket creation to resolve the incident and restore service to the user.

Target Percentage of Calls Resolved on Time:
The percentage of calls that meet the priority time frame criteria.

2.9 Priority Chart

Priority	Target Incident Response Acknowledge-ment Time	Target Status Update Interval	Customer Status Update Interval	Target Resolution Time	Target % of Calls Resolved on Time
1	15 minutes	Every 15 minutes	CSC will update every 30min	4 clock hours or less	90% rising to 95% within first 6 months of rollout; Reassess target at end of 6 months
2	30 minutes	Within 1 hour	CSC will	8 clock hours	90% rising to

Priority	Target Incident Response Acknowledge-ment Time	Target Status Update Interval	Customer Status Update Interval	Target Resolution Time	Target % of Calls Resolved on Time
		then every hour thereafter	update every 2 hours	or less	95% within first 6 months of rollout; Reassess target at end of 6 months
3	2 hours	Within 3 hrs	Upon request	24 clock hours or less	80% rising to 85% within first 6 months of rollout; Reassess target at end of 6 months
4	1 business day	Within 1 business day	Upon request	3 business days	80% rising to 85% within first 6 months of rollout; Reassess target at end of 6 months
5	1 business day to acknowledge receipt of request / order	SLA or as agreed upon with Customer	Upon request	SLA or as agreed upon with Customer	SLA or as agreed upon with Customer

2.10 Customer Notification

ITS will provide all communications via the following means: online ticket updates, phone calls, and/or email notifications utilizing the customer contact information (see Customer Responsibilities).

2.11 Escalation Contact List

The ITS Customer Support Center is the Single point of contact for all incidents to be reported to ITS. Please contact the ITS Customer Support Center (CSC) at **919-754-6000** or toll free at **1-800-722-3946** to report any incidents or to initiate service requests. Contact may also be made by emailing the CSC at ITS.Incidents@ncmail.net.

If there is reason to believe that the incident or request is not being handled appropriately or if additional questions need to be answered about ITS services, their business value or ITS Processes, contact the Business Relationship Manager assigned to your agency

If this does not satisfactorily resolve the issue please contact the Director of Business Relationship Management, Wendy Kuhn. Subsequent escalations, where necessary should be to Deputy State CIO, Bill Willis and then State CIO, George Bakolia

At any time the Business Relationship Manager can be called to help explain ITS services or work with the business team on information technology business needs.

3 Customer Responsibilities

ITS and the Agency will work together to make sure that all responsibilities can be met. Below are responsibilities for which ITS will need support and ownership from the Agency:

- Follow appropriate incident reporting procedures for ITS operational incidents including cyber security incidents.
- Identify critical business systems and applications.
- Work with ITS to implement agency data classification and handling measures based on legal and regulatory requirements.
- Provide emergency contact information for key agency personnel that may be needed during a cyber security incident.
- Request and schedule special services (for example, installation of new equipment, after-hours support) well in advance.
- Be aware of and comply with the State CIO Security Standards, Policies and procedures and ITS agency level policies for ITS services provided (email, network etc.)
- Be willing and available to provide critical information to assist in the resolution of reported incidents.
- Appoint qualified staff to support information security measures.
- Access and manage agency information security risk.
- Appropriately staff agency level information security business support functions.
- Define appropriate agency internal security policies, standards and procedures.
- Work with ITS to provide appropriate security training to agency staff.
- Work with ITS to define agency internal information security incident plans, policies and procedures.
- Integrate agency internal information security incident plans with the statewide security incident plan.
- Work with ITS to provide internal agency security incident response oversight.
- Develop and follow agency level project plans to implement agency level security.

4 Performance and Service Level Reviews

A basic goal of ITS management is to keep the customer regularly informed. Status meetings, status reports, performance measurements, and planning sessions are the vehicles used to ensure that the Customer is kept apprised of activities. ITS management believes that to provide effective services to the customers, management must maintain awareness of events and make effective use of all resources. This will position ITS to meet the service level commitment to our customers.

Monthly - There will be a monthly meeting with the Agency and the Business Relationship Manager from ITS providing a scorecard to the agency of the performance of ITS services.

Semi-Annually (or as needed) – There will be a semi-annual performance review with the Agency, State CIO and Business Relationship Manager from ITS. This discussion will provide information on performance by ITS in providing the service outlined in this SLA. This will also be used to make ITS aware of business events or changes that may impact or change the services provided by ITS.

Yearly – There will be a yearly service review meeting to provide metrics and measurement to determine if the service level requirements have been met for the agency. If requirements are not met or partially met then improvement areas will be developed with action plans for changes to improve the service.

The SLA will also require review under any of the following conditions:
1) Whenever there is a significant and/or sustained change to the delivery of the Information Security Threat Management and Incident Response Services
2) Whenever there is a significant and/or sustained change requested to the SLA that supports the Information Security Threat Management and Incident Response Services Services.

5 Security Standards and Policies

This SLA is in compliance with ITS and State CIO Security Standards and Policies.

6 Business Continuity Plan

This SLA is supported by a Business Continuity Plan as specified in ITS ISO Business Continuity Plan. Agency responsibilities should be documented in a corresponding agency business continuity plan.

7 Dispute Resolution for Service Impacting Outages or Failure to Perform

ITS and the agency agree that it is in their mutual interest to resolve disputes informally. When there is a dispute about a "service impacting outage" or a failure in performance occurs, the Agency Secretary or Agency Deputy Secretary shall contact the State Chief Information Office (CIO). A report shall be prepared that identifies the underlying cause and a remediation action plan shall be developed and agreed upon by both agencies. The State CIO and Agency Secretary or Agency Deputy Secretary shall meet and discuss any changes needed to be made by either ITS and/or the agency. If the agency is not satisfied with the resolution, the agency may refer the matter to the Office of State Budget and Management for its review and recommendation.

8 Metrics and Reports

Report name	Reporting Metric	Reporting interval	Reporting Source	Delivery method
Incident and Request Time to Repair Analysis	Percentage of requests and incidents resolved within target timeframe, minus lost time	Monthly	iWise	Email
Incident and Request Resolution Performance	Mean time to Repair - MTTR minus lost time resolved within target time frame	Monthly	iWise	Email

Archival of all reports shall follow the records retention schedule adopted by the North Carolina Office of Information Technology Services and the State Records Branch General Schedule, as applicable.

9 Definitions

Terminology	Description
Business Relationship Manager	Position in ITS that works the senior management of a agency go help provide understanding and foster business relationships between ITS and the agency.
Customer Support Center	Central team that is the single point of contact for agency customers to report problems or request services from ITS.
Cyber Security	The discipline of Security working with digital data or information technology.
Emergency Maintenance Windows	A timeframe where IT infrastructure will be taken out of service to fix a problem that is outside of the normally scheduled maintenance timeframe.
Incidents	A failure in hardware, software or services that results in a customer not being able to utilize technology.
Information Security Office	The Information Security Office (ISO) under the direction of the State Chief Information Security Officer provides leadership in the development, delivery and maintenance of an information security program that safeguards the state's information assets and the supporting infrastructure against unauthorized use, disclosure, modification, damage or loss.
ISO 17799	The only Internationally recognized comprehensive Information Security Standard. It is the basis for the state security standards.
iWise	ITS IT Service Management tool used to track work within ITS including incidents, problems, requests, and changes.
Mean Time To Repair (MTTR)	The average amount of time, it takes to restore/repair service. This includes prime time and weekend and holiday guarantees.
Schedule Maintenance Windows	A timeframe where IT infrastructure is taken out of service for maintenance. This is done with knowledge and approval from the customer.
Threat Management	Process to identify exploits such as malicious code that could compromise the confidentiality, integrity and availability of an information resource and define appropriate measures to respond to and mitigate these risks
Vulnerability Management	Process to identify defects in hardware and software that could be exploited to compromise an IT system and to define plans to repair these defects before they become a threat.

10 Signatures of Approval

Agency Secretary or Deputy Secretary:

Name	Title	Signature	Date

ITS Senior Management**:**

Name	Title	Signature	Date

Appendix A: Supported Hardware and Software

Supported hardware

The following hardware is supported:

This hardware is located at the ITS Data Center and is used to evaluate security.

Hardware services

The following hardware services are provided:

This hardware is located at the ITS Data Center and supported by ITS.

Unsupported hardware

The following are representative, but not comprehensive, examples of hardware that is *not* supported:

Door alarm systems, badge control systems, security hardware that may be agency specific which is not supported by ITS.

Software Services

ITS agrees to cover software support services, including software installations and upgrades for the software listed in “Supported Software.”

Supported software

The following software and applications are supported:

Security Software used for forensic investigation, intrusion detection and prevention and virus management is supported by ITS.

Unsupported software

The following are representative, but not comprehensive, examples of software that is *not* supported:

Application security programs and software used for door alarm or badge control systems.

Appendix B: Information Security Threat Management and Incident Response Services Special Amendments

None at this time.